Software Reliability and Safety

CSE 8317 — Fall 2005

Prof. Jeff Tian, tian@engr.smu.edu
CSE, SMU, Dallas, TX 75275
(214) 768-2861; Fax: (214) 768-3085
www.engr.smu.edu/~tian/class/8317.05f

OV.2. Review

- QA Alternatives/Activities and Their Relation to CSE 8317

- Fault Tolerance in SSE: SQE Ch.16a

- Common Techniques: SQE Ch.20 & 21

Review: QA Alternatives

- Defect prevention/removal/tolerance
  - ▷ SQE/slides online:
    - Part I (particularly Chapter 3)
    - Parts II and III (high-level only)
- Defect prevention:
  - ▷ Error source elimination
  - ▷ Error blocking
- Defect removal: Inspection/testing/etc.
- Defect tolerance:
  - ▷ Fault tolerance (failure↓)
  - ▷ Damage minimization (safety)

QA Alternatives and 8317

- SRE relation/applications:
  - ▷ QA alternatives directly work with SRE
  - ▷ Functional relation: reliability $\sim$ failure
  - ▷ Remember? error $\Rightarrow$ fault $\Rightarrow$ failure
  - ▷ All will affect the end results/failures
  - ▷ Closer to failure
    $\Rightarrow$ closer to SRE activities
    (e.g., system and acceptance testing)

- SSE relation/applications:
  - ▷ More focused (not as broad)
  - ▷ Hazard focus (small subset of failures)
  - ▷ Specifics to be examined later

QA Alternatives and 8317

- Inspection:
  - ▷ Good throughout dev. process
  - ▷ Works on many software artifacts
  - ▷ Conceptual/static faults
  - ▷ High fault density situations
  - ▷ Human intensive, varied cost

- Applications in SRE and SSE
  - ▷ Fault eliminations:
    – helps both reliability and safety
  - ▷ Scenario-based inspection:
    – for SRE – common usage scenarios
    – for SSE – FTA/ETA-based scenarios/elements
  - ▷ Early reliability prediction
  - ▷ Safety constraints and inspection
  - ▷ Leveson's process-based approach

QA Alternatives and 8317

- Formal verification: SQE Ch.15
  - ▷ Works on code with formal spec.
  - ▷ Practicality: high cost → benefit?
  - ▷ Human intensive, rigorous training

- Applications in SRE and SSE
  - ▷ High cost ⇒ most in SSE
  - ▷ Module SSE.3
  - ▷ Focus through FTA and/or ETA
  - ▷ Leveson's approach:
    – safety and other constraints
    – carried through dev. process
  - ▷ Other adaptations:
    – table-driven, model checking, etc
    – PSC, module SSE.4

QA Alternatives and 8317

- Testing:
  - ▷ Important link in dev. process
  - ▷ Activities spilt over to other phases
    – OP/testcase development
  - ▷ Dynamic/run-time/interaction problems
  - ▷ Test tools and execution support
  - ▷ Technique: analysis/behavior-based
  - ▷ Coverage vs. reliability focus

- Applications in SRE and SSE
  - ▷ Chief application domain for SRE
  - ▷ OP-based testing:
    – basis for reliability modeling
  - ▷ Indirect link to SSE

QA Alternatives and 8317

- Fault tolerance:
  - ▷ Dynamic problems
  - ▷ Technique problems (independent NVP?)
  - ▷ Process/technology intensive
  - ▷ High cost

- Applications in SRE and SSE
  - ▷ Too expensive for regular SRE
  - ▷ As hazard reduction technique in SSE
  - ▷ Other related SSE techniques:
    - – general redundancy
    - – substitution/choice of modules
    - – barriers and locks
    - – analysis of FT

QA and Safety

- Hazard elimination through defect prevention and removal

- Reduce fault injection
  - ▷ General: education/process/tech./etc
  - ▷ Specific: better software designs
    - – complexity↓
    - – decoupling
    - – certified components, etc.
  - ▷ Formal specification & verification
    - – focus on safety req. & assertions

- Fault removal focused on safety
  - ▷ Static/dynamic analyses (FTA/ETA/more)
  - ▷ Rigorous/focused testing (earlier)
  - ▷ Inspection and verification (earlier)

QA and Safety

- Hazard reduction through
  - ▷ Redundancy (fault tolerance)
  - ▷ Process and safety standards, etc.
  - ▷ General barriers and safety margins
- Hazard control
  - ▷ Isolation and containment
  - ▷ Protection system
  - ▷ “active”
  - ▷ Typically beyond traditional QA
- Related: post-accident damage reduction (typically beyond traditional QA)

Specialized QA for Safety

- Focused formal verification in connection with hazard analysis
  - ▷ Only safety-critical part formally verified
  - ▷ Combination of different techniques
  - ▷ Safety-constraints driven

- Fault tolerance ⇒ hazard tolerance
  - ▷ Safety vs. operational concerns
  - ▷ If problem, shut down but safe
    – vs. operation with reduced capacity
  - ▷ SQE Ch.15a

- Ideas into Leveson's SSP:
  integration into development process.